WATERMARKING PADA DOMAIN FREKUENSI UNTUK MEMBERIKAN IDENTITAS (WATERMARK) PADA CITRA DIGITAL

Zaki Rakhmatulloh, Aris Sugiharto, Eko Adi Sarwoko
Jurusan Matematika FMIPA UNDIP
Jl. Prof. Soedarto, Kampus UNDIP Tembalang, Semarang

Abstrak: *Watermarking* merupakan salah satu solusi dalam memecahkan penggandaan ilegal produk digital. Pada penelitian ini *watermarking* citra digital ditransformasikan menggunakan *discrete cosine transform* (*DCT*). Pada proses penanaman *watermark*, citra ditransformasikan menggunakan *DCT* menjadi domain frekuensi yang menghasilkan tiga area yaitu *Low Frequency* (*FL*), *Medium Frequency* (*FM*), dan *High Frequency* (*FH*). Bit-bit *watermark* ditanam pada area *FM* dengan menggunakan nilai Koefisien Selisih (K). Kualitas citra ter-*watermark* diukur dengan *Peak Signal of Noise Ratio* (*PSNR*). Semakin besar nilai K diperoleh nilai *PSNR* yang semakin kecil.

Kata Kunci: *watermarking*, *watermark*, *DCT*, *PSNR*

PENDAHULUAN

Selama ini penggandaan atas produk digital, seperti citra digital dilakukan begitu bebas dan leluasa secara ilegal. Hasil penggandaan tersebut memiliki kualitas yang sama dengan produk digital aslinya. Namun, pemegang hak cipta produk digital tidak mendapatkan royalti dari usaha penggandaan diatas, akibatnya pemegang hak cipta produk digital dirugikan atas usaha ilegal di atas.

Hampir semua produk digital yang tersebar di internet jarang mencantumkan informasi pemiliknya. Salah satu produk digital yang tersebar di internet adalah citra digital. Seseorang yang telah mendapatkan citra digital dapat mengklaim bahwa citra digital tersebut adalah hasil karyanya. Karena jika tidak ada bukti kepemilikan citra digital sebelumnya, maka setiap orang dapat mengklaim citra digital tertentu sebagai miliknya.

Berbagai upaya dilakukan untuk melindungi citra digital dari upaya penggandaan secara ilegal. Salah satunya adalah dengan *watermarking*, pada penggunaan *watermarking* akan disisipkan sebuah *watermark* sebagai identitas dari pemilik citra digital yang sah. Pemberian *watermark* dilakukan tanpa merubah citra digital secara langsung sehingga keberadaannya tidak merusak citra digital yang dilindungi. Jika seseorang membuka citra digital yang telah disisipi *watermark*, maka orang tersebut tidak akan menyadari bahwa di dalam citra tersebut telah terkandung label kepemilikan pembuatnya. Sebuah label *watermark* akan selalu terbawa kemana saja citra digital tersebut berada termasuk hasil penggandaannya. Jika dikemudian hari ada orang lain yang mengklaim bahwa citra digital tersebut adalah miliknya, maka pemegang hak cipta tersebut dapat membantahnya dengan cara mengekstrak kembali *watermark* dari citra digital yang disengketakan. Jika *watermark*-nya sama dengan yang dimiliki oleh pemegang hak cipta, maka orang tersebut merupakan pemegang hak cipta citra digital yang sebenarnya.

TINJAUAN PUSTAKA

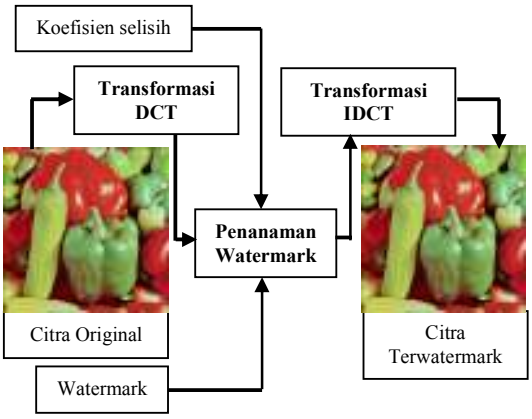
Watermarking

Watermarking merupakan suatu bentuk dari *Steganography*. *Steganography* adalah ilmu yang mempelajari bagaimana menyembunyikan suatu data pada data yang lain [6]. Sehingga seseorang tidak menyadari kehadiran adanya data tambahan pada data tersebut. Jadi seolah-olah tidak ada perbedaan antara data sebelum dan sesudah proses *watermarking*. Disamping itu data yang ter-*watermark* harus tahan (*robust*) terhadap serangan-serangan baik secara sengaja maupun tidak sengaja untuk menghilangkan data *watermark* yang terdapat didalamnya.

Watermarking memanfaatkan kekurangan-kekurangan sistem indera manusia seperti mata dan telinga. Sehingga *watermarking* juga dapat didefinisikan sebagai suatu cara penyembunyian data atau informasi tertentu ke dalam suatu data digital lainnya, tetapi tidak diketahui kehadirannya oleh indera penglihatan atau indera pendengaran manusia dan mampu menghadapi proses-proses pengolahan signal digital sampai pada tahap tertentu [2].

Terdapat dua proses dalam *watermarking*, yaitu proses penyisipan dan proses pengekstrakan. Proses penyisipan adalah proses menyisipkan *watermark* ke dalam citra digital yang akan disisipi. Untuk menyisipkan suatu *watermark* ke dalam citra digital, diperlukan bilangan selisih (K). K merupakan bilangan yang menjadikan *pixel*-

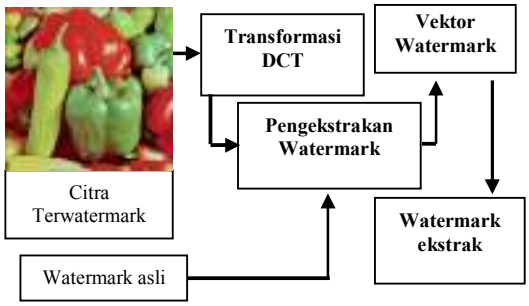
pixel yang telah ditukar antara dua blok yang telah ditentukan sebagai area penanaman *watermark* memiliki selisih tertentu.



Gambar 1. Proses Penyisipan *Watermark*

Sedangkan proses pengekstrakan adalah proses mengekstrak kembali *watermark* yang telah tertanam pada citra terwatermark.

Untuk proses pengekstrakan dibutuhkan *watermark* asli dari citra ter-*watermark* sebagai pembanding ukuran dalam membentuk kembali *pixel-pixel watermark* yang telah ditanamkan dalam citra ter-*watermark*.



Gambar 2. Proses Pengekstrakan *Watermark*

Sifat dan Manfaat Watermarking

Untuk mendapatkan suatu digital watermarking yang baik, maka teknik yang digunakan memenuhi sifat-sifat di bawah ini [2] :

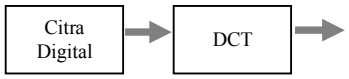
1. Tidak tampak (*Invisible)* untuk data digital seperti citra oleh pihak lain dengan menggunakan panca indera terutama indera penglihatan.
2. Tidak mudah dihapus atau diubah secara langsung oleh pihak yang tidak bertanggung jawab, dan tidak mudah terhapus atau berubah dengan adanya proses pengolahan sinyal digital.
3. Tidak menghambat proses penduplikasian tetapi penyebaran data digital tersebut tetap dapat dikendalikan dan diketahui.

Ada beberapa manfaat yang dapat dicapai dari penggunaan watermarking, sebagai suatu penyembunyian data pada data digital lain [1], yaitu:

1. *Tamper-proofing*
   Watermarking digunakan sebagai alat indikator yang menunjukkan data digital asli telah mengalami perubahan dari aslinya (mengecek integritas data).
2. *Feature location*
   Watermarking sebagai alat identifikasi isi dari data digital pada lokasi-lokasi tertentu, misalnya penamaan suatu objek tertentu dari beberapa objek yang ada pada suatu citra digital.
3. *Annotation/caption*
   Watermark hanya digunakan sebagai keterangan tentang data digital itu sendiri.
4. *Copyright-Labeling*
   Watemarking digunakan sebagai metoda untuk menyembunyikan label hak cipta pada data digital atau sebagai bukti autentik kepemilikan atas dokumen digital tersebut.

Discrete Cosine Transform (DCT)

Transformasi pada *watermarking* digunakan untuk menyederhanakan penyelesaian dan untuk mengetahui suatu informasi tertentu yang tidak tersedia sebelumnya.. *Discrete cosine transform* (*DCT*) memecah citra digital menjadi blok-blok kecil dengan ukuran yang tetap kemudian dikonversikan dari domain spatial menjadi domain frekuensi. *Discrete cosine transform* (*DCT*) merekonstruksi matrik citra ke dalam tiga area frekuensi yaitu *Low Frequency* (*FL*), *Medium Frequency* (*FM*), dan *High Frequency* (*FH*) [3].



Gambar 3. *Discrete cosine transform* (*DCT*)

Peak Signal to Noise Ratio (PSNR)

Peak Signal to Noise Ratio (PSNR) merupakan nilai (rasio) yang menunjukan tingkat toleransi *noise* tertentu terhadap banyaknya *noise* pada suatu sinyal citra. *Noise* adalah kerusakan sinyal pada bagian tertentu dalam sebuah citra sehingga mengurangi kualitas sinyal tersebut. Dengan kata lain *PSNR* merupakan suatu nilai yang menunjukkan kualitas suatu sinyal citra. [7]

Untuk menentukan nilai *PSNR* digunakan rumus :

$$PSNR = 20 * \log 10 \left(\frac{255}{\sqrt{MSE}}\right)$$

Sedangkan *MSE (Mean Square Error)* adalah kesalahan kuadrat rata-rata sinyal-sinyal piksel citra hasil pemrosesan sinyal terhadap sinyal citra asli. Rumus untuk menghitung *MSE* pada citra digital adalah sebagai berikut [4]:

$$MSE = \frac{1}{MN} \sum_{y=1}^{M} \sum_{x=1}^{N} [I(x,y) - I'(x,y)]^2$$

(untuk Citra Grayscale)

$$MSE = \frac{1}{3MN} \sum_{i=1}^{3} \sum_{y=1}^{M} \sum_{x=1}^{N} [I(x,y)_i - I'(x,y)_i]^2$$

(untuk Citra RGB)

dimana :

M	: Baris matriks citra hasil pemrosesan.
N	: Kolom matriks citra hasil pemrosesan.
$I'(x,y)$	: Piksel citra hasil pemrosesan.
$I(x,y)$	: Piksel citra asli.
i	: index matriks (*Red* = 1, *Green* = 2, dan *Blue* = 2).

PEMBAHASAN

Metode

Pada penelitian ini semua bahan yang digunakan adalah citra digital yang mudah diperoleh di berbagai media. Metode yang digunakan dapat digambarkan sebagai berikut :

Pertama, citra original disisipi citra *watermark* menghasilkan citra terwatermark. Kualitas citra terwatermark ini kemudian diuji dengan parameter yang digunakan adalah *Peak Signal to Noise Ratio (PSNR)*.

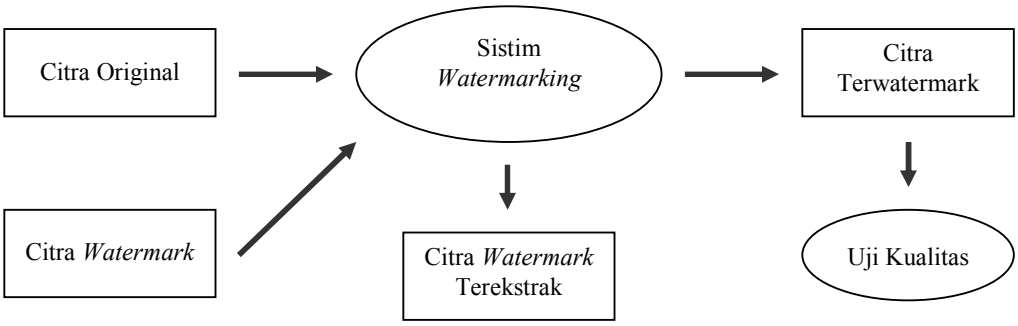
Selanjutnya citra terwatermark yang telah diketahui nilai PSNR, diekstrak menghasilkan citra *watermark* terekstrak. *Watermark* terekstrak ini hanya digunakan sebagai pembanding kemiripan secara visual dengan citra *watermark* asli.

Metode ini dilakukan berulang-ulang dengan konstanta transformasi yang berbeda-beda.

Citra digital dengan nilai *PSNR* tertentu dapat dikategorikan ke dalam 5 kategori sebagai berikut [7]:

Tabel 1. Nilai *PSNR*

PSNR (dB)	Picture Quality
60	Excellent, no noise apparent
50	Good, a small amount of noise but picture quality good
40	Reasonable, fine grain or snow in the picture, some fine detail lost
30	Poor picture with a great deal of noise
20	Unusable



Gambar 4. Uji Kualitas Citra Terwatermark

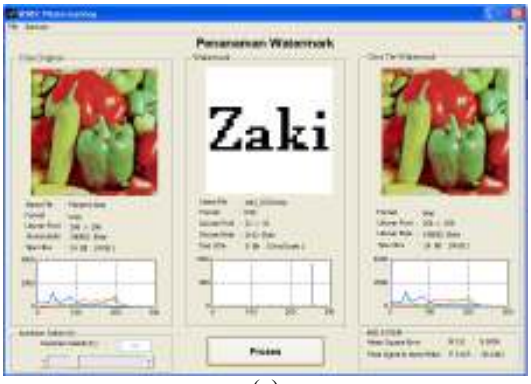
Hasil

Citra yang disimulasikan adalah citra *Peppers.bmp*, berukuran 256 x 256 piksel, dengan jenis citra *RGB* 24 bit. Sedangkan citra *watermark*-nya adalah citra *zaki_3232.bmp* berjenis *grayscale* 8 bit, berukuran 32 x 32 piksel.

(a) (b)

Gambar 5. (a) Peppers.bmp, (b) zaki_3232.bmp

Kedua citra di atas kemudian disimulasikan dalam sistem *watermarking* dengan menggunakan *Graphical User Interface (GUI) MATLAB 7.1* [5] yang diperlihatkan pada gambar 6.



(a)

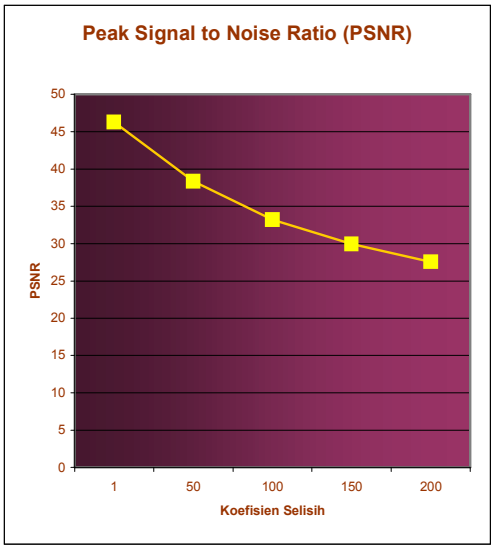
(b)

Gambar 6. (a)Penyisipan/Penanaman Watermark, (b)Pengekstrakan *Watermark*

Gambar 6 (a) adalah simulasi proses penyisipan citra *watermark* ke dalam citra asli. *PSNR* citra ter-*watermark* (citra asli yang telah tersisipi *watermark*) dapat terlihat pada panel *Catatan Proses* pada tampilan simulasi. Sedangkan gambar 6 (b) adalah simulasi proses pengekstrakan kembali *watermark* yang telah tersisipi pada citra ter-*watermark*.

Pengujian dengan menggunakan Koefisien selisih (K) 1, 50, 100, 150, 200 diperoleh hasil *PSNR* dan *watermark* terekstrak sebagaimana pada Tabel 2.

PSNR yang diperoleh dapat digambarkan dalam bentuk grafik sebagai berikut :



Gambar 7 . Grafik *PSNR DCT*

Tabel 2. Nilai PSNR dan Watermark ekstrak

Koefisien Selisih (K)	DCT	
	PSNR*	Watermark Terekstrak
1	46.2751	
50	38.3492	Zaki
100	33.204	Zaki
150	29.9508	Zaki
200	27.5787	Zaki

PSNR : PSNR untuk citra terwatermark*

Grafik pada gambar 7 menyatakan hubungan antara koefisien selisih (K) dengan *Peak Signal to Noise Ratio* (*PSNR*). Angka-angka pada absis X menunjukkan skala K, sedangkan pada ordinat Y menunjukkan skala *PSNR*.

Dari grafik terlihat garis bergerak menurun dari kiri ke kanan. Hal ini berarti bahwa semakin besar nilai K yang digunakan dalam proses penyisipan *watermark*, maka akan berpengaruh pada penurunan nilai *PSNR*. Dengan kata lain semakin besar nilai K yang digunakan, maka semakin menurun kualitas citra ter-*watermark*.

Sedangkan pada proses ekstraksi, secara *visual* dapat terlihat bahwa nilai K berpengaruh pada *watermark* ekstrak. Semakin besar nilai K yang digunakan, maka akan semakin mirip *watermark* yang terekstrak dengan *watermark* asli.

PENUTUP

Dari hasil yang diperoleh pada penelitian ini maka dapat disimpulkan bahwa semakin besar koefisien selisih (K) yang digunakan dalam proses transformasinya, berakibat pada semakin menurunnya kualitas citra ter-*watermark*, tetapi secara visual citra *watermark* ekstrak semakin mirip dengan citra *watermark* asli..

DAFTAR PUSTAKA

[1]. Bender, W. Gruhl, D. Morimoto, N. Lu, A., Techniques for Data Hiding, *IBM System Journal*, Vol.35, 1996.

[2]. H. Supangkat, dkk, *Paper* : *Watermarking sebagai Teknik Penyembunyian Label Hak Cipta pada Data Digital*. Institut Teknologi Bandung. 2000.

[3]. Langelaar, G. Setyawan, I. Lagendijk, R.L., Watermarking Digital Image and Video Data, in *IEEE Signal Processing Magazine*, Vol. 17, pp. 20-43, 2000.

[4]. Li Tan, Choo, *Still Image Compression using Wavelet Transform*, School of Information Technology and Electrical Engineering, The University of Queensland. Queensland. 2001.

[5]. Littlefield, Bruce and Duane Hanselman, *MATLAB Bahasa Komputasi Teknis*, Andi and Pearson Education Asia Pte, Ltd., Yogyakarta. 2000.

[6]. Schneiner, B., *Applied Cryptography: Protocols, algorithm, and Source Code in C*, New York: Wiley, 1994.

[7]. www.cctv-information.co.uk/constant2/ sn_ratio.html

[8]. www.mathworks.com